サイバー保険のニーズが急速に高まり、保険会社や再保険会社にとって大きな商機が訪れているが、業界として大きな損失をこうむる恐れもある。リスク評価、リスク算定、リスク移転の仕組みを構築し、サイバー保険を持続可能な商品に育てるにはどうすればよいのだろうか?

Insurance 2020 & beyond:
サイバー保険に関する展望

pwc

www.pwc.com/jp

目次

はじめに：
リスクを冒す価値があるか？

PwCの『Insurance 2020 & beyond』シリーズ[1]の最新版では、「サイバー保険に関する展望」を取り上げる。

サイバー保険は保険会社や再保険会社にとってはほとんど未開拓の巨大分野だ。現在25億米ドル[2]の年間の総収入保険料は、10年以内に75億米ドル[3]まで成長する見込みだ。

複雑化が進み、リスクが高まる今日の環境においては、サイバー保険の重要性が業種を問わずあらゆる企業に認識されるようになった。保険会社や再保険会社はこれを価格競争が激化している市場の中で高いマージンを得る貴重な機会と見て期待を寄せている。サイバーリスクの引受けに二の足を踏んでいる会社もまだ多いが、このような様子見をいつまで続けていられるだろうか。近い将来にはクライアントからサイバー保険が求められるようになり、サイバー保険を扱わない保険会社は見向きもされなくなる恐れもある。

既に多くの保険会社は、IT業務賠償責任保険、過失怠慢賠償責任（E&O）保険、総合賠償責任保険などの既存分野において大きなサイバーリスクにさらされている。「見えない」リスクを評価し管理することが急務だ。

大きなリスク

サイバー保険に懐疑的な見方がこれほど強いのはなぜだろうか。その理由の1つは、サイバーリスクが他のリスク保険会社や再保険会社がこれまで引き受けてきたリスクとはまったく異質なものだという点にある。攻撃の規模や財務的影響に関しては、ごく限られたデータしかない。また、脅威の進化と拡散のスピードが速いことも手をつけにくい要因だ。保険会社は合理的な確証に基づいてシステム復旧のコストを見積もるが、ブランドの失墜や、クライアント、サプライヤー、その他の関係者への補償に伴うさらなる損失を計算するための過去のデータが不足している（必要となる新しいシナリオベースの手法については後述する）。英国政府の報告書では、保険業界の世界規模でのサイバーリスクエクスポージャー（保証の総額）は既に1000億ポンド（1500億米ドル）規模に達しており[4]、戦略国際問題研究所が推計するサイバー攻撃の年間損失額（4000億米ドル）[5]の3分の1を超えている。潜在的損失額の規模は自然災害と同程度だが、発生率は大幅に高い。その結果、サイバーリスクが集中することと、経験の浅い保険会社が立て続けに起こる高額の損失に対応できるかどうかを懸念する声が高まっている。

1 www.pwc.com/insurance/future-of-insurance and www.pwc.com/projectblue

2 ロイズ会長John Nelson氏のAAMGAでのスピーチ、2015年5月28日（https://www.lloyds.com/lloyds/press-centre/speeches/2015/05/vision-2025-and-aamga）

3 PwCによる推計（10ページを参照）

4 'UK Cybersecurity: The role of insurance in managing and mitigating the risk', UK Government, March 2015

5 'Net Losses:Estimating the Global Cost of Cybercrime', Centre for Strategic and International Studies, June 2014.
この報告書では、年間損失額は「控え目に見積もって3750億米ドル」、「最大で5750億米ドル」、「4000億米ドル以上の見込み」と推計されている。

「サイバーリスクの引受けはロイズシンジケートにとって商機ではあるが、適切な管理が行われなければ市場に重大なリスクが集中する恐れがある。また、サイバーリスク保険の保険料が適切に設定されていない、あるいは管理関係者によってリスクが十分に定量化されていない可能性も懸念される」

Tom Bolt氏（ロイズ、業績管理担当ディレクター）[6]

保険会社および再保険会社は不確実性を織り込んで、サイバー保険の保険料を他の賠償責任保険よりも高く設定している。また、潜在的損失額を抑えるため、制限事項や除外事項、条件も付けている。しかし、そのような保険契約にどれほどの実用的価値があるのかが多くのクライアントに疑問視されるようになれば、市場の成長が妨げられる可能性がある。

強固な基盤

本書では、どのようにすればサイバー保険の事業としての持続性を高め、クライアントに真の保護を提供し、保険会社および再保険会社がこうむる損害を軽減することができるかを探る。

例えば、信頼性の高いデータに基づいて厳密かつ適正なリスク評価、効果的なシナリオ分析を行い、政府やIT企業、専門家との連携を強化する必要がある。保険会社は包括保険契約に頼ってリスクをコントロールするのではなく、クライアントの事業運営の定期的なリスク評価や、定期検証で浮上した課題への対応策を条件として保証を行う。評価の深さはクライアントの業界のリスクや適用範囲に応じたものとする。

このように緻密な情報に基づくアプローチを採用することで、不測のリスクを低減するとともに、クライアントの要望に応えた保険の提供や保険料の抑制が可能になる。保険の透明性とコスト効率を高めることは、クライアントにとってもメリットとなる。

最後に、バランスシート保護を強化する方法の他、従来の再保険と資本市場構造を組み合わせた効果的なリスク移転方法も探る。最後に、サイバーリスクに関連して、セキュリティを強化するにはどうすればよいかを考える。保険会社はクライアントに関する膨大な量の機密情報を保有しているため、サイバーリスク市場で信頼性を維持し、企業として信頼を得るには、効果的な保護策が不可欠だ。

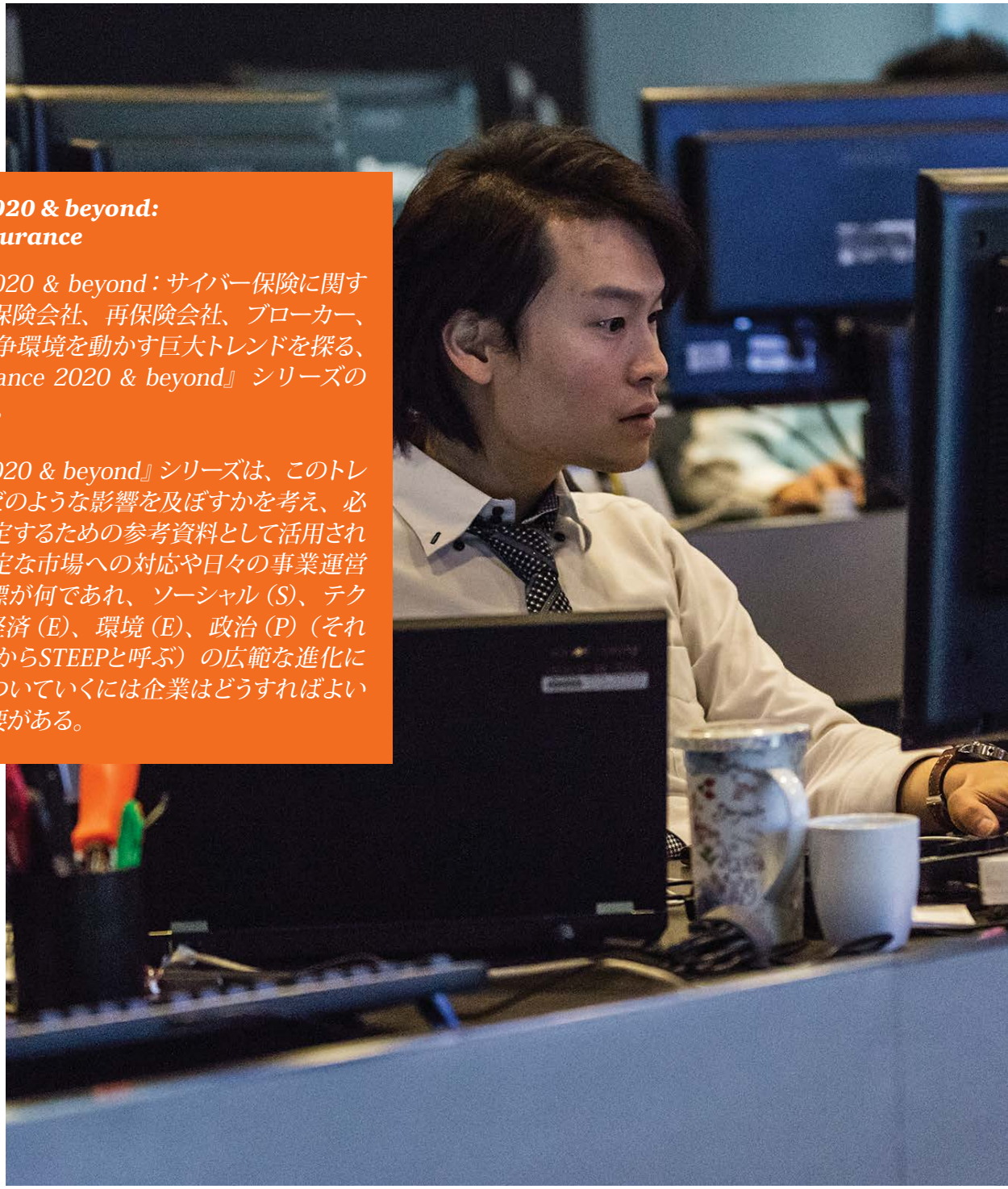
このように持続性を考慮したアプローチを支えるのは、文化、人材、プロセス、ITといったあらゆる面から総合的にサイバーリスクをとらえる姿勢である。PwCはこれを「サイバーレジジリエンス」と呼んでいる。

本書で取り上げた内容の詳細については、PwCの担当者までお問い合わせください。

最大のリスク：最新のインシュアランス・バナナ・スキン調査によると、損害保険会社はサイバーリスクを自社にとっての最大のリスクと見ている[7]。

6 Lloyd's Market Bulletin, 25 November 2014

7 Insurance Banana Skins 2015には54カ国から806の業界関係者が参加しインタビューを受けた。インシュアランス・バナナ・スキンは、金融イノベーション研究センター（CSFI）がPwC（http://www.pwc.com/insurancebananaskins）と協力して実施している業界リスクの独自調査である。



Insurance 2020 & beyond:
Future of insurance

『Insurance 2020 & beyond：サイバー保険に関する展望』は、保険会社、再保険会社、ブローカー、保険市場の競争環境を動かす巨大トレンドを探る、PwCの『Insurance 2020 & beyond』シリーズの最新版である[8]。

『Insurance 2020 & beyond』シリーズは、このトレンドが企業にどのような影響を及ぼすかを考え、必要な戦略を策定するための参考資料として活用されている。不安定な市場への対応や日々の事業運営など、短期目標が何であれ、ソーシャル（S）、テクノジー（T）、経済（E）、環境（E）、政治（P）（それぞれの頭文字からSTEEPと呼ぶ）の広範な進化に後れを取らずついていくには企業はどうすればよいかを考える必要がある。

8 www.pwc.com/insurance/future-of-insurance およびwww.pwc.com/projectblue

1

サイバーに関する脆弱性：異質なリスク

サイバーリスクの課題には、従来のリスク評価やリスク算定、リスク管理が通用しない

デジタル革命によりあらゆるものが相互につながるようになった結果、不正使用や窃取、漏洩の恐れのある機密データがあふれている。加えてマルウエア、（D）DoS攻撃などの悪意ある攻撃、サイバーリスクが大きな脅威として私たちの生活を脅かしている。

サイバー犯罪者は絶えず弱点を探り、さまざまな手を繰り出してくる。攻撃元は活動家や犯罪組織などであると思われがちだが、従業員が犯罪に手を染めることも多い。標的の幅も広がっている。保険業界でも、物資輸送の追跡データを狙って企業がハッキングされた事例が出てきた。

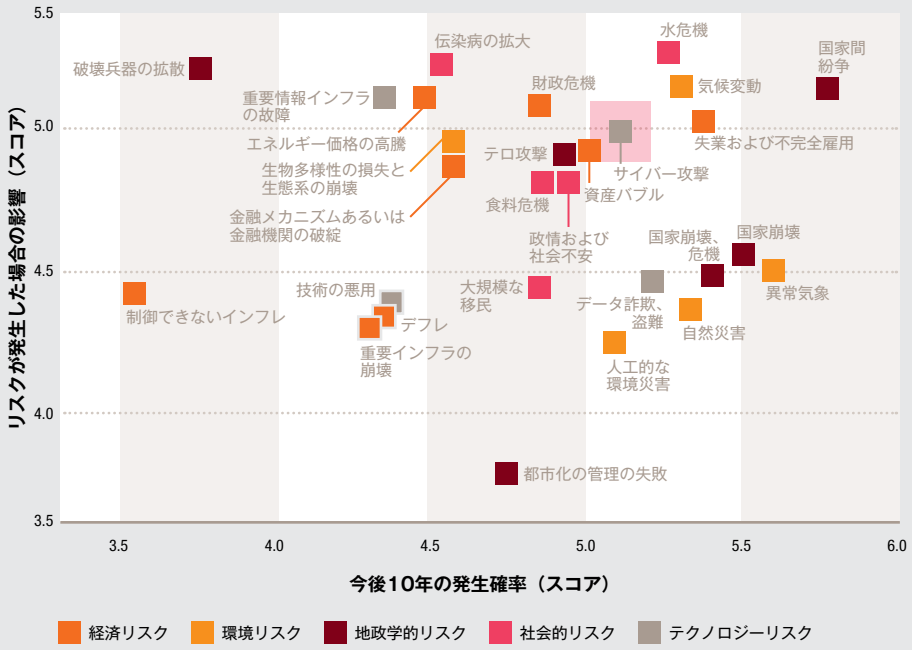
このように、サイバー犯罪は被害が大きく検知が困難で、手ごわい脅威だ。テロや災害のリスクに例えられることも多いが、保険の観点から見てサイバーリスクは異質であると言える。

サイバー犯罪は世界経済に年間4000億米ドル以上[9]の損害を与えており、被害はさらに拡大中である

9 'Net Losses: Estimating the Global Cost of Cybercrime', Centre for Strategic and International Studies, June 2014.
この報告書では、年間損失額は「控え目に見積もって3750億米ドル」、「最大で5750億米ドル」、「4000億米ドル以上の見込み」と推計されている。

保険会社のCEOの71%、銀行CEOの79%、全業界のビジネスリーダーの61%が、消費者行動の変化、ITの変革スピード、サプライチェーンの機能停止よりも成長を脅かす要因としてサイバー攻撃を挙げている[10]。

図1：グローバルリスクの影響と発生確率



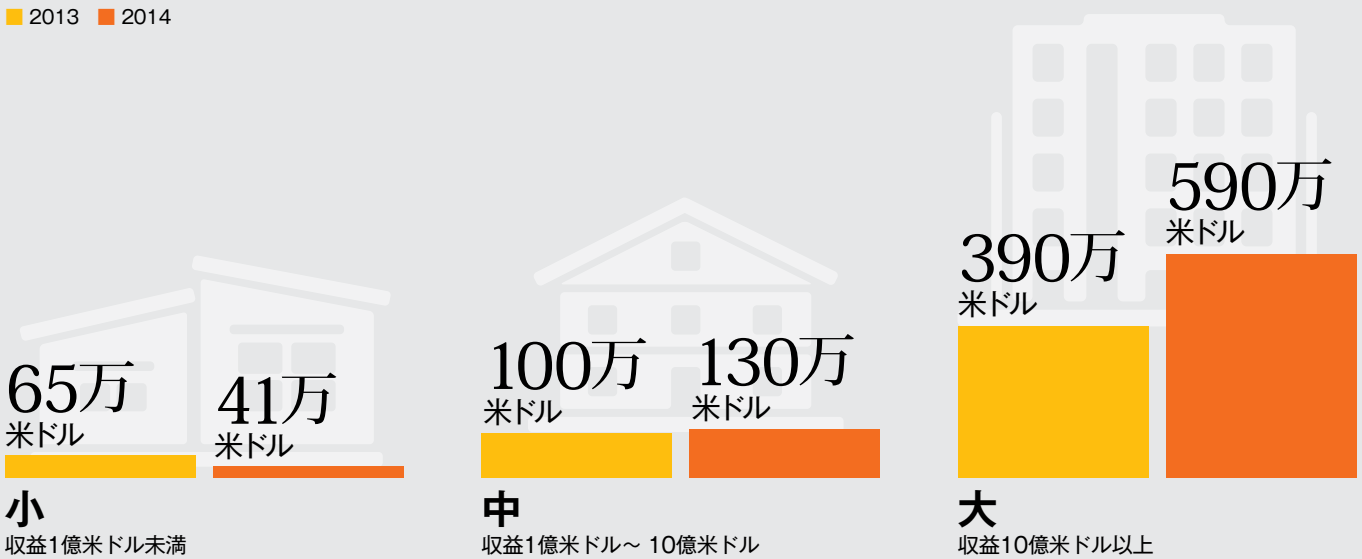
注：調査では個々のリスクの発生確率と影響度を1 ～ 7の数字で評価するよう求めた（発生確率および影響度は最小で1、最大で7とした）。

出典：World Economic Forum ‘Global Risks, 10th Edition’, 2015

1　発生確率は高く、影響も深刻

図1のように、サイバーリスクは影響も発生確率も高いスコアを示している。セキュリティ、IT、ビジネスエグゼクティブを対象としてPwCが毎年実施している調査では、2014年に世界で検知されたセキュリティインシデントは4300万件近くに上った[11]。これは1日10万件以上の攻撃に相当する。財務的影響は上昇の一途をたどっており（図2）、数千万米ドル規模に達しているものもある。保険会社が多額の損失を立て続けにこうむれば、破滅的事象後の影響を吸収したり、これまでと同様の収益を上げたりすることが困難になる恐れがある。

図2：インシデントのコストは大企業ほど高い
セキュリティインシデントによる平均的な財務的損失額（2013年～ 2014年）



出典：『相互につながった世界におけるサイバーリスクマネジメント：グローバル情報セキュリティ調査2015』PwC[11]

2　損失の広がりを抑えにくい

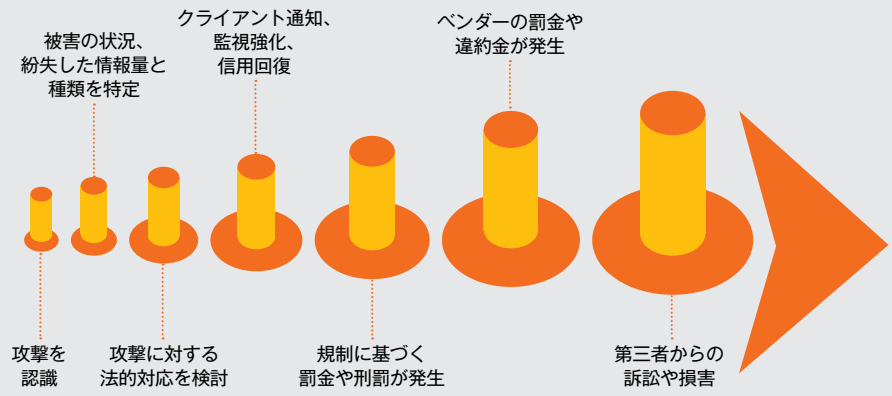
影響は業務の中断やシステムの修復だけにとどまらない。罰金や訴訟、評判の低下なども加わる。図3は、サイバー攻撃を受けた場合の影響が長引き、予想がつかないことを示している。企業が参加するエコシステムのつながりと依存がますます強まる中では、自社のシステムとデータのみではなく、サプライヤー、クライアント、戦略的パートナーもともに危険にさらされることになる。IoT（モノのインターネット）の登場によって接続性が高まるとともに、脆弱性も拡大した[12]。企業が使用するインフラストラクチャーへの攻撃も危惧される。

3　リスクの検知、評価、算定が困難

サイバー攻撃の財務的影響に関する実務データは限られている。そのため、コストを正確に算定することは容易ではない。ITシステムのバックアップを作成し、火事や洪水で停止した場合に復旧させるためのコストを見積もることは可能だが、ブランドの失墜、クライアント、サプライヤー、その他の関係者への補償に伴うさらなる損失を見積もるにはデータがあまりに不足している。この不確かさに加え、サイバーセキュリティ侵害が月単位、あるいは年単位で検知されないまま放置され、将来にかけて複合的な累積損失が生じる可能性もある。

サイバー保険単体を提供していなくても、財産保険、事業中断保険、総合賠償責任保険、過失怠慢賠償責任（E&O）保険に広く存在するリスクを測定することが必要だ。請求を制限する除外事項がある場合もあるが、徹底的な検証を行うことが望ましい。

図3：サイバー攻撃の影響は長引き、予想がつかない



出典：PwC

保険会社には舵取り役が期待されている

サイバーリスクは拡大中であり、未知の要素が多く、被害額も大きい。このリスク管理の究極の責任者は誰だろうか。

経営陣は大きな損害を引き起こすサイバー攻撃に対する保護策の必要性を認識しつつある。サイバー保険はリスク移転のための選択肢の1 つだ。サイバー保険商品によって生じた収益成長機会を積極的にとらえた保険会社は多いが、リスクが大きすぎて引き受けられないと判断している保険会社もある。また、テロや洪水など、補償が困難な場合と同様に、政府が最後の手段として保険または再保険を手がけるかどうかも取り沙汰されている。しかし、話を聞く限り、多くの政府関係者にとって望ましいのは、政府が設定した基準に従って構成され管理された営利保険であるようだ。サイバー攻撃が国家の支援を受けている場合も、これを戦争行為と宣言するのは躊躇されるため、特定の除外条項が行使される。

サイバーリスクを明示的に引き受けないという選択も可能だ。ただし、前述のとおり、既存の保険契約に既にリスクが存在する可能性がある。やがてサイバー保険が主流になれば、長年のクライアントやブローカーから直接的あるいは暗に求められるようになるかもしれない。従って、好むと好まざるとにかかわらず、少なくともサイバーリスク補償を事業計画に取り入れる必要があるだろう。

10 PwCが実施した第18回 世界CEO意識調査（www.pwc.com/ceosurvey）で1,322人のCEOにインタビュー

11『相互につながった世界でのサイバーリスクマネジメント：グローバル情報セキュリティ調査2015』、PwC（http://www.pwc.com/gx/en/consulting-services/information-security-survey）

12 'Insurance 2020 & beyond：必要性が再び改革を生み出す'、PwC、2015（www.pwc.com/insurance2020reinvention）

2

サイバー保険市場の成長：持続可能な解決策の必要性

保険会社は厳しい保険約款と保守的な保険料算定でサイバーリスクを抑えるしかない。しかし、クライアントが保険契約の価値に疑問を抱くようになり、市場がサイバーリスクのレベルや集中に危惧を抱くようになったとき、このアプローチはどの程度通用するだろうか?

サイバー保険が収益成長の大きな機会であることは間違いない。2014年に引き受けたサイバー保険の保険料は25億米ドルと推定されている[13]。サイバー保険の加入者の約90%は米国企業であり[14]、さらに世界へと拡大する市場の規模は明らかだ。例えば英国では、単体サイバー保険に加入している企業はわずか2%にすぎない[15]。加入が進んでいる米国市場でも、何らかのサイバー保険を利用している企業は3分の1程度だ[16]。また、加入度は業界によっても大きく異なる。単体サイバー保険に加入している米国の企業は、医療、IT、小売業界では50%前後であり、製造業ではわずか5%だ[17]。サイバー脅威の認識が高まるにつれ、取り組みが遅れていた業界や国での加入が増加し続けている。また、企業はサイバー保険への加入状況を開示する必要に迫られている(米国証券取引委員会の開示ガイダンス[18]など)。このような状況から、サイバー保険の年間保険料は2018年までに50億米ドル、2020年までに少なくとも75億米ドルまで成長が見込まれる。

各保険会社は、サイバー保険引受けの拡大に強い意欲を見せている。全体的に価格競争が激しい他の領域と比べ、高い保険料が期待できるからだ。一般的に、サイバー保険の購入限度額に対するコストは、従来の一般賠償責任保険の3倍だ[19]。料金が高いのは、潜在的損失に備えてどれくらいの引当金が要るのかが不透明であり、扱っている保険会社の数も少ないからだ。

また、多くの保険会社が設定している限度額は、クライアントが求める金額に届かない(最大5億米ドル。多くの大手保険会社では3億米ドル以下[20])。制限付きの除外事項や条件を課すこともある。最新のデータ暗号化やセキュリティパッチの更新を100%とすることなどの条件を守ることは企業にとっては困難だ。高い保険料、支払限度額、条件の厳しさ、請求に関する制限事項などを考えると、保険加入者にとって現実的な価値があるのかどうかを疑問視する声も多い。このような懸念は、目下の成長を阻害する要因となる。また、過度に厳しい契約条件を課せば、規制措置や訴訟を招きかねない。

13 ロイズ会長John Nelson氏のAAMGAでのスピーチ、2015年5月28日(https://www.lloyds.com/lloyds/press-centre/speeches/2015/05/vision-http://www.lloyds.com/2025-and-aamga)

14 Fortune, 23 January 2015

15 Reuters, 23 March 2015

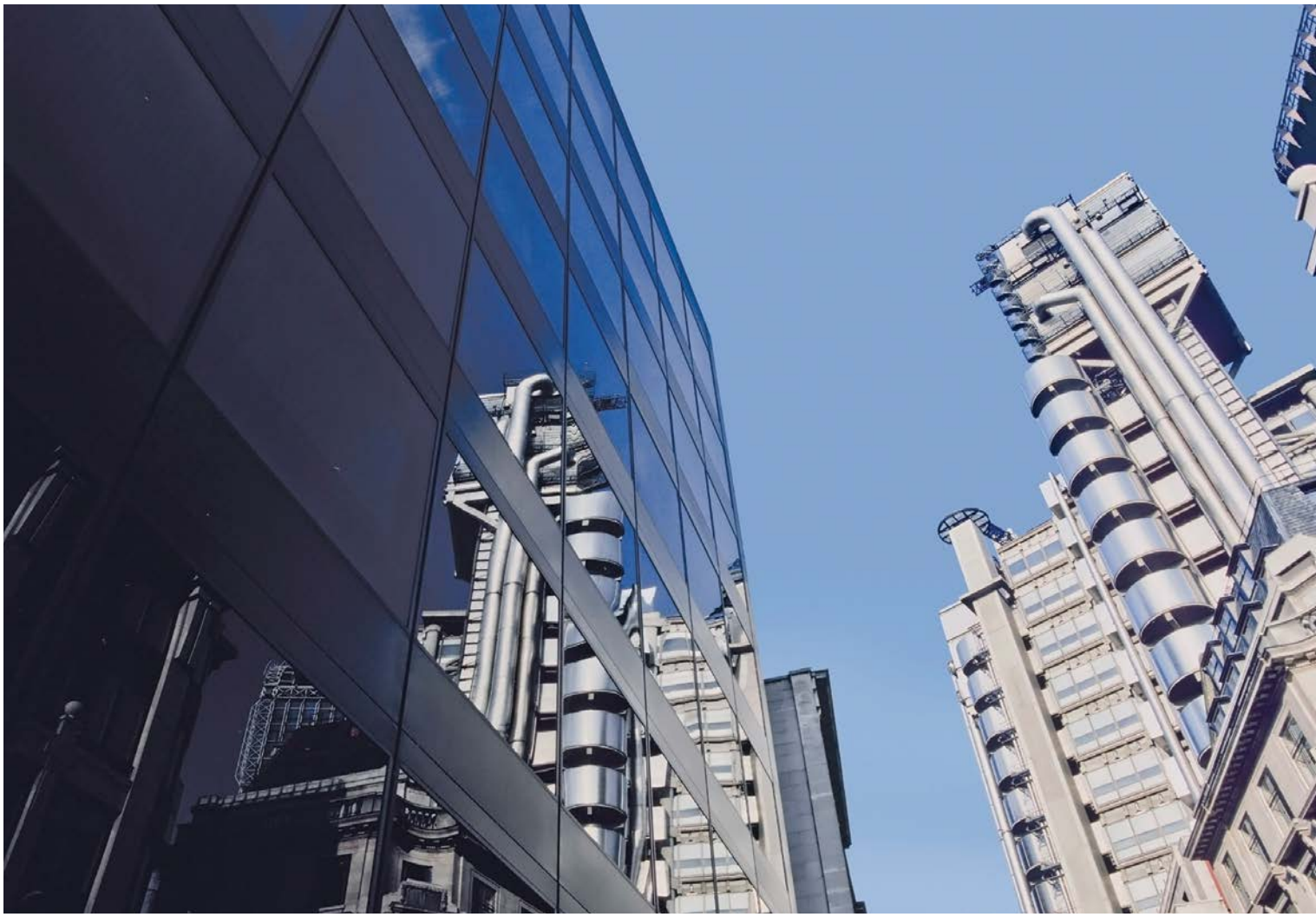
16 Aon Benfield Insurance Risk Study 2014

17 Willis Insights, March 2014

18 https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

19 'UK Cybersecurity: The role of insurance in managing and mitigating the risk', UK Government, March 2015

20 Financial Times, 18 February 2015



広がる懸念

制限や条件、除外事項を使って潜在的損失を抑えても、多くの規制機関や市場ではサイバーリスクの累積や集中がなおも危惧されている。

サイバー保険を扱う大手保険会社が多く拠点を置く英国では、規制機関の動きが目立つ。2014年11月、ロイズはリスク集約および管理プロセスの監視を強化する対策を打ち出した。これによって、必要な場合に的を絞った介入が可能になる[21]。2015年7月には、英国Prudential Regulation Authority（PRA）が60以上の保険会社に対し、データ漏洩や集団訴訟につながる[22]多国同時サイバー攻撃に基づいてシナリオ分析を行うよう要請した。

この動きは、潜在的損失を十分に理解していない、または耐えられない保険会社がサイバー保険をこれ以上引き受けられないよう、規制機関が乗り出してくる明確な兆候だ。

失われる余裕

サイバー保険の規模は今後数年にわたり膨らみ続け、保険料水準を押し下げる可能性が高い。競争原理が働き、保険会社による制限や除外事項などの条件も緩和されるだろう。

さらに将来に目を向ければ、市場はやがて成熟し、データに基づいて料率を正確に設定できるようになる。そうすれば、不確実性を保険料に反映する必要性は薄れる。問題は、そうなるまでにどれくらいの時間がかかるのか、そしてこの動きを加速できるのかどうかだ。あまりに時間がかかるようであれば、価格破壊者が大胆な低価格や加入者に有利な条件で市場に参入してくる恐れがある。

21 Lloyd's Market Bulletin, 25 November 2014
22 General Insurance Stress Test 2015

3

サイバーサステナビリティ：適切な場所に十分な保護を

サイバーリスクを機にビジネスを拡大すると同時にリスクを管理するには、リスク評価、リスク算定、リスク移転の新しいアプローチが必要だ。

PwCでは、保険会社、再保険会社、ブローカーがサイバー保険を持続可能な商品として育て、時代の波に乗って収益性を高めるには、次の8つの方法があると考えている。

1　許容できる損失を見極める

保険料を科学的に算定できるのは、しっかりとした保険数理があってこそだ。合計最大損失がさらに明確になれば、リスク選好度やリスク許容度と照らし合わせることも可能だろう。どの業界に注力すべきか、どのようなときに保険引受を縮小すべきか、拡大余地がどこにあるかを見極めるのに役立つ。

投入する情報として重要なのは、ポートフォリオのワーストケースシナリオ分析だ。例えば、クライアントに米国電力会社が多い場合、米国の送電網が大規模な攻撃を受けたらどのような損失をこうむるだろうか。高度な技術を持つハッカーグループが米国の送電網に侵入するという「発生し得るが可能性は低い」シナリオに基づいた最新レポートでは、保険会社が受ける請求は攻撃の規模と範囲によって210億米ドルから710億米ドルに上ると推計されている[23]。この請求額のうち、保険会社が支払うべきはどれくらいだろうか。損失を抑えるためには、どのような対策をとればよいだろうか。ポートフォリオのリスク集中を軽減する、クライアントの保護策や危機対応計画を強化するといった対応が考えられる。

2　情報収集を強化する

脅威評価やクライアントの脆弱性評価を効果的に行うためには、IT企業や情報機関の力を借りることが重要だ。リスク評価、スクリーニング、保険料算定のプロセスが確立されれば、保険数理士や保険会社は補償や第三者損害賠償責任保険に、またITエキスパートはデータやシステムの領域に専念できるようになる。協力してサイバー脅威に立ち向かうために、CROチームとCIOチームがそれぞれの役割を果たすのと同じことだ。

23 'Business Blackout: Emerging risk report 2015', Lloyd's, 7 July 2015

3　リスクベースの条件

現在は保険会社が一括的に条件を課していることが多いが、保険加入者のアセスメントの範囲と頻度を増加させることを条件に補償を行う方が効果的だ。これには、クライアント企業のプロセス、責任、ガバナンスの監査も含まれる。また、政府機関などの信頼できる情報源から業界や特定の企業に対する脅威評価を得て、脅威情報の評価も行う。演習として模擬攻撃も行い、弱点をテストして対策を練る。補償条件として、予防および検知のための適切なテクノロジーや手順の実装を求めるのもよいだろう。

保険会社は受容するリスクを深く理解してコントロールできるようになり、エクスポージャーの縮小と適切な保険料を実現できる。クライアントにとっても、コスト効率よく効果の高い保険を付保することができるという利点がある。このような評価を行うことで、クライアントとの関係を縮めて強化し、フィーベースのアドバイザリーサービスの基盤も構築できる。

4　情報共有を進める

効果的な情報共有を実現するには、保険料算定の精度を向上する必要がある。クライアント企業は評判低下を恐れ、データ漏洩をなかなか認めない。保険会社は競争力を失うことを懸念してデータを共有したがらない。しかし、米国で始まったデータ漏洩の報告を義務付ける法律がEUにも広がり、今後は使用可能なデータが増加しそうだ。データ共有イニシアチブを開始した政府や規制機関もある（シンガポールのMAS、英国のサイバーセキュリティ情報共有パートナーシップなど）。ORIC（Operational Risk Consortium）を通じて運用リスクに関するデータを蓄積することで、業界全体での共有が進む。

対応準備を整える

画面が赤く光るのを見て、CEOの額に汗が噴き出した。ITセンサーは犯罪組織からサイバー攻撃を受けていることを示している。CEOはチームを率いて、攻撃を阻止する方法を見つけ出し、次の攻撃に備えなければならない。CEOの頭の中をさまざまな考えが駆け巡る。実装しているセキュリティシステムで敵を食い止められるだろうか。攻撃者が繰り返しサイバー防御を破って侵入を試みる中、固唾をのんで状況を注視する。画面を見ると、攻撃はいずれも阻止されている。攻撃者は最後にランサムウエアの起動を試みた。そこですばやくマルウエアをリバースエンジニアリングし、事なきを得た。CEOは安堵のため息をもらし、椅子に倒れこんだ。

これはシミュレーションだが、いつ現実のものになってもおかしくない。脆弱性と対応準備状況を測る効果的な方法として、このような仮想演習を導入する例が増えている。PwCがクライアント向けに開発したシミュレーション演習では、個々の業界や企業に対する最新の脅威情報評価に基づいてシナリオを構築している[24]。経営陣がサイバー防御力をテストして強化するとともに、意思決定の方法や順序を変えるとどのような違いが生じるのかを把握するためだ。この違いこそが戦略的に重要な意味を持つ。クライアントの情報収集と保護を強化することで、保険会社はクライアントのリスク評価を改善して個々の状況に応じた契約条件を提案するとともに、サイバー関連の損失を縮小できる。

5　保険契約をリアルタイムで更新

年に一度の更新と18カ月の商品開発サイクルでは、リアルタイム分析を行い短い間隔で保険契約を更新する企業に勝つことはできない。この積極的なアプローチと、セキュリティソフトウエアの更新、または信用保険会社のアプローチを組み合わせて、限度額とエクスポージャーを臨機応変に管理する。

6　ハイブリッド型のリスク移転

サイバー再保険市場は一般的な保険と比べて発展が遅れているが、進化する脅威と最大損失シナリオをより深く理解することで、再保険企業の市場参入が進む可能性がある。

24 PwC Game of Threats (http://www.pwc.com/us/en/financial-services/cybersecurity-privacy/game-of-threats.html)

自社すら守れない保険会社が、保険加入者の信頼を得られるだろうか

リスク移転構造には従来から続く下位層での超過損害再保険が含まれることが多い。資本市場構造では最大損失が考慮されている。選択肢としては、免責や業界損失保証の仕組み、あるいは不測の事態に備えた資本などが考えられる。このような資本市場の仕組みは、多様化と利益を求める投資家にとって魅力的だろう。ファンドマネジャーや投資銀行が再保険会社やIT企業の専門知識を生かせば、適切な評価手法が生み出される。

7　リスクの斡旋

サイバーリスクがこれまでにないほど複雑化し、損失要因が不透明になるとともに、企業、保険会社／再保険会社、資本市場、政府などのさまざまな関係者が協調してリスク管理に取り組むことが求められるようになっている。ブローカーのようなリスク斡旋者が関係者をまとめ、多くの政府が乗り気になっているサイバー保険の標準などの効果的な解決策の策定を主導する必要があるだろう[25]。

8　効果的な社内の保護策を通じて信頼を獲得

サイバーリスク市場で信頼性を維持し、企業として信頼を得るには、効果的な社内の保護策を開発することが不可欠だ。自社すら守れない保険会社が、保険加入者の信頼を得られるだろうか。

銀行はサイバーセキュリティに何億米ドルもの投資を行い。情報機関から人材や元ハッカーを招いて、保護策に関する助言を受けている[26]。扱っている機密情報の量を考えれば、保険会社も後に続くのは時間の問題だ。ひとたびデータ漏洩が起これば、失った信頼を取り戻すことは非常に難しい。サイバー保険を扱う保険会社が持つ機密データのうち、ハッカーに狙われやすいのは、クライアントのサイバーリスクおよび防御策に関する情報だ。

経営陣が第一に求められることは、ITやコンプライアンスの問題ととらえるのではなく、自らが率先してサイバーリスクの評価と対策に取り組むことだ（図4を参照）。

25 課題の詳細については、「Broking 2020: Leading from the front in a new era of risk」（http://www.pwc. com/gx/en/insurance/reinsurance-rendezvous/insurance-2020.jhtml）を参照

26 Cyber insecurity: When 95% isn't good enough, Financial Times, 28 July 2015

図4：サイバーセキュリティはITだけの問題ではない

出典：PwC

保護を強化するために自問すべき点：

- 自社にとっての敵は誰か？攻撃の標的は何で、どのような影響が考えられるか？（図5を参照）
- 全てを停止することができないことを前提として、保護すべき最重要資産は何か？
- 自社のプロセスや責任の割り当て、システムの保護策の有効性はどの程度か？
- 脅威情報や分析評価を積極的にサイバー防御プログラムに組み込んでいるか？
- 既知の攻撃手法や攻撃ツールに対して脆弱性を評価しているか？

これらの疑問点に対する答えを明らかにすることで、リスク認識を高め、組織全体での対応を強化して、サイバーレジリエンスを向上できる。このレジリエンスを実現してこそ、将来の技術発展の恩恵を確実に享受し、イノベーション、コラボレーション、生産性、カスタマーエクスペリエンスを向上することが可能になるのだ。

図5：脅威および脆弱性の評価

	目的	ターゲット	インパクト
敵対国家	・経済や政治、軍事的優位性の確立 ・国際社会における信頼や評判の低下	・取引機密、企業機密情報 ・最新テクノロジー ・重要基盤 ・注目される大規模イベント	・競争的優位性の損失 ・重要基盤の崩壊 ・社会的混乱 ・国家や組織の信頼低下
組織犯罪	・即時の金銭獲得 ・将来的な金銭獲得目的の情報収集	・金融/決済システム ・個人証明情報 ・支払カード情報 ・保護された医療情報	・規制による調査/罰金 ・顧客/株主による訴訟 ・顧客からの信頼の失墜
ハクティビスト	・政治および社会変化への影響 ・企業へプレッシャーをかけることによる、ビジネス変更	・企業機密情報 ・役員/従業員/カスタマー/ビジネスパートナとの関係情報 ・重要な財務システム	・規制による調査/罰金 ・訴訟 ・ビジネス活動の破壊 ・ブランド/評判の低下 ・顧客からの信頼の失墜
インサイダー	・個人的な利益、金銭獲得 ・仕事上の復讐 ・贈賄/強要	・営業/マーケティング戦略 ・企業機密情報/知的財産/研究開発情報 ・個人情報 ・社内システムの認証情報	・機密情報の漏洩 ・経営の混乱 ・ブランド/評判の低下

出典：PwC

4

結論：差別化と成果

料金設定や制限条件が横並びである市場においては、サイバーリスクを深く理解しコントロールすることが、明確な差別化による競争力と持続可能な利益につながる。より魅力的な保険料と引受け条件を提案できること、効果的なリスク移転を実現できることが優位性となる。

まず取り掛かるべきことは、保険請求が発生する具体的な状況と、サイバー脅威を考慮に入れていない保険契約の潜在的リスクレベルの特定だ。

次に、シナリオ分析を行い、脅威情報を積極的に収集し、クライアントのリスクを積極的に低減する。このような取り組みを通じて、効果的にリスクを評価しコントロールできる。

ただし、従来の賠償保険のような信頼度や精度をもって保険料を設定することは至難の業だ。しかし、豊富な情報に基づく持続可能なサイバー保険モデルを開発することで、不透明性を保険料に反映する必要は薄れ、資金を効率的に割り当てて再保険の利用や資本市場へのリスク移転を検討できる。また、保険引受けを調整し、特定の市場を狙いやすくもなる。

デジタル化の波に乗り、成長著しいサイバー保険市場のリーダーとなるには、自社のサイバーセキュリティを確立することが不可欠だ。重要なのは、サイバーリスクをシステムやITの問題ではなく、企業全体の問題としてとらえることだ。経営陣が指揮を執り、事業運営にサイバーレジリエンスを組み込むことが肝要である。

保険会社や再保険会社の間では、サイバーリスクを懸念する声も根強い。その一方で、大きなリスクを引き受ける会社もある。スマートな分析手法、機敏な対応、リスク移転といった取り組みにより、自社を危険にさらすことなく事業を運営できるようになるだろう。

お問い合わせ先

プライスウォーターハウスクーパース株式会社
03-3546-8480（代表）

松崎 真樹
パートナー
maki.matsuzaki@jp.pwc.com

山本 直樹
パートナー
naoki.n.yamamoto@jp.pwc.com

PwCサイバーサービス合同会社

星澤 裕二
パートナー
yuji.hoshizawa@jp.pwc.com

www.pwc.com/jp

本報告書は、PwCメンバーファームが2015年9月に発行した『Insurance 2020 & beyond: Reaping the dividends of cyber resilience』を翻訳したものです。翻訳には正確を期しておりますが、英語版と解釈の相違がある場合は、英語版に依拠してください。

電子版はこちらからダウンロードできます。 www.pwc.com/jp/ja/japan-knowledge/thoughtleadership.html
オリジナル（英語版）はこちらからダウンロードできます。 http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

日本語版発刊月：2015年12月　　管理番号：I201510-5